Journal: Government Computer News Sep 23, 1996 v15 n24 p55(2)

Title: The Netscape Biscuit Company serves up a snack that knows you. (Hypertext Transfer Protocol cookies)(Internaut) (Internet/Web/Online Service Information)

Author: McCarthy, Shawn P.

Abstract: Hypertext Transfer Protocol 'cookies' are now being used by Webmasters to monitor who and how their Web sites are accessed so that they can custom-tailor their page presentations. Agencies such as the SEC can make use of cookies as a tool for improving service to repeat site visitors. To create a cookie, Web servers should be set up to populate a database with visitor information or to build a data string in the visitor's browser that can be retrieved later. Among the information that a server can automatically pick up are IP address, time of access, pages visited and user preferences. With an optional online form, other data can be gathered, to be sorted and compresed by a CGI script into a character string. There is an active cookie embedded in Netscape's Navigator 2.0 or 3.0 browser.

Full Text:

Pour yourself a glass of milk. Let's talk about cookies and what they mean to government World Wide Web sites.

Persistent-client-state Hypertext Transfer Protocol "cookies" in client browsers can tell Web servers specific things about the users who access them. Cookies have been around for more than a year, but only recently have webmasters used them to track usage and custom-tailor their page presentations.

Cookies can be a powerful tool for serving repeat visitors. For instance, a Securities and Exchange Commission site could recognize visitors and sort its filings the way they want them--by company name, transaction amount or date. A government contracting office site could consult a cookie and immediately display the visitor's account status plus a checklist of deliverables.

Preheat the oven

Here's how you mix cookies. You set up the Web server to populate a database with information about a visitor or to create a data string that's stored in the visitor's browser for later retrieval---or a combination of the two,

The server automatically picks up basic information such as IP address, time of visit, user preferences and pages visited. Other information can be collected with an optional on-line form.

When a form is filled in, a Common Gateway Interface (CGI) script sorts the information and compresses the results into a character string, little more than a single line, for storage in the browser's cookie file. This can hold all the collected information or just a series of keys to

trigger retrieval of other information from the server's database.

If you use a Netscape Communications Corp. Navigator 2.0 or 3.0 browser, you probably have an active cookie set stored on your desktop machine. Look for the file called COOKIES.TXT in your Netscape folder. It will list the Internet address of each server that has modified your file, followed by a string of settings used by that server.

Add nuts and chips

I'm willing to bet you'll find entries from FOCALINK.COM or DOUBLECLICK.NET, which coordinate the display of on-line advertising and use cookies to track who's seen what, so the same ad isn't encountered at every turn. I've found cookie entries from Netscape and a Microsoft Windows NT site on my machine.

The cookie functionality originally built into Netscape 2.0 is blossoming under the new Version 3.0, mainly because some security holes were patched. One noticeable difference is that you can set the 3.0 browser to notify you when your cookie file is being modified.

Where cookies turn most delicious yet potentially dangerous is in their ingredients-the information can be abused. Netscape's Commerce Server platform, for example, allows virtual malls where visitors put chosen items into their "shopping carts," actually cookie files that track the items for payment.

Burned

A cookie contains only information you've given, or general IP information that can be collected by any Web server, nothing more. But cookies are getting a bad reputation for possibly holding a lot of information that users don't want shared with everyone.

Although there really isn't anything secret in your cookie file, servers can read and write to it. If they can decipher another server's cryptic cookie string, your information could, in theory, be passed along without your knowledge or consent.

A larger problem arises when cookies are combined with JavaScripts--tiny programs sent to a browser whenever a particular page is requested. These scripts perform tasks such as scrolling text and launching applets.

Hackers have written JavaScripts to retrieve a user's e-mail address or to scout for certain activity from the Netscape cache file, which documents a user's movements on the Web. A hacker could easily use JavaScript to steal or alter cookie information. The safest way to use cookies is with the RSA Data Security Inc. encryption feature built into Netscape Navigator.

To develop cookies, you must have a product that lets you integrate edited Hypertext Markup Language code into template files and database table fields. Don't tackle this unless you have solid Structured Query Language and database administration knowledge.

Two products that come to mind are Cold Fusion Professional from Allaire Corp. of Minneapolis, a $495 Web authoring package, and WebDBC from Nomad Development Corp. of Seattle, a $595 set of Internet/Web server tools.

Samples and packages

Microsoft Corp.'s Internet Explorer also supports many cookie functions, although I've heard complaints that the implementation isn't identical.

Programmers sometimes end up creating different types of cookies for different browsers. Netcom On-line Communications Services Inc.'s NetCruiser and Quarterdeck Corp.'s Quarterdeck Mosaic 2.0 also offer some cookie support.

For a brief introduction to cookies, visit Netscape's page at http://www.netscape.com/ newsref/std/cookie_spec.html. For a look at how they work, visit Live Software's simple cookie demo at http://jrc.livesoftware.com/ cookies/page2.html.

Shawn P. McCarthy is a computer journalist, webmaster and Internet programmer for GCN's parent, Cahners Publishing Co. E-mail him at smccarthy@cahners.com.

Type: Column
Topic: Internet/Web Technology

Record#: 18 741 091

*** End ***